Docket No. AUS920010544US1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Kaply et al.**

Serial No. **09/884,493**

Filed: **June 18, 2001**

For: **Method and Apparatus for Removing Confidential Information from a History**

§ Group Art Unit: **2174**

§ Examiner: **Vu, Thanh T.**

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, facsimile number (571) 273-8300 on November 8, 2005.

By: Michele Morrow
Michele Morrow

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on September 8, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-4, 6-16, and 18-24.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 5 and 17.
2. Claims withdrawn from consideration but not canceled: NONE.
3. Claims pending: 1-4, 6-16, and 18-24.
4. Claims allowed: NONE.
5. Claims rejected: 1-4, 6-16, and 18-24.
6. Claims objected to: NONE.

C. CLAIMS ON APPEAL

The claims on appeal are: 1-4, 6-16, and 18-24.

STATUS OF AMENDMENTS

There are no amendments after the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 11, 13, and 23:

The present invention provides a method in a data processing system for removing information. (Specification, page 13, lines 13-28) The present invention receives a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser. (Specification, page 19, line 21 to page 23, line 11, and page 19, lines 7-11) The present invention identifies data elements, within the history, that correspond to the confidential information that has been selected. (Specification, page 19, lines 11-13) The present invention automatically removes the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history in response to a termination of the browser session. (Specification, page 9, lines 13-20)

The system recited in claim 11 may be a bus system comprised of bus system **206**; communication unit **222**, memory **204**, and processing unit **202** performing the steps described in the specification at page 19, line 1, to page 23, line 11, or equivalent. The means recited in independent claim 13, as well as dependent claims 14-16, 18, and 19, may be data processing hardware within computer **100** in **Figure 1** operating under control of software performing the steps described in the specification at page 19, line 1, to page 23, line 11, or equivalent. A person having ordinary skill in the art would be able to derive computer instructions on a computer readable medium as recited in claim 23 given **Figures 9-12** and the corresponding description at page 19, line 1, to page 23, line 11, without undue experimentation.

Independent claims 8, 12, 20, and 24:

The present invention provides a method in a data processing system for removing information from a history generated by a browser. (Specification, page 13, lines 13-28) The present invention receives a selection of confidential user information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser. (Specification, page 19, lines 7-11 and page 19, line 21 to page 23, line 11) The present invention identifies data elements, within the history, that correspond to the confidential information that has been selected. (Specification, page 19, lines 11-13) The present invention removes the selected confidential information from the history in response to generation of the history, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history. (Specification, page 19, lines 13-20)

The system recited in claim 12 may be a bus system comprised of bus system **206**; communication unit **222**, memory **204**, and processing unit **202** performing the steps described in the specification at page 19, line 1, to page 23, line 11, or equivalent. The means recited in independent claim 20, as well as dependent claims 21 and 22, may be data processing hardware within computer **100** in **Figure 1** operating under control of software performing the steps described in the specification at page 19, line 1, to page 23, line 11, or equivalent. A person having ordinary skill in the art would be able to derive computer instructions on a computer readable medium as recited in claim 24 given **Figures 9-12** and the corresponding description at page 19, line 1, to page 23, line 11, without undue experimentation.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. GROUND OF REJECTION (Claims 1-4, 7-16, and 19-24)

Claims 1-4, 7-16, and 19-24 are rejected under 35 U.S.C. § 102(e) as being allegedly anticipated by Qian et al. (U.S. Publication No. 2002/0032731).

B. GROUND OF REJECTION (Claims 6 and 18)

Claims 6 and 18 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Qian et al. (U.S. Publication No. 2002/0032731) and Barnett et al. (U.S. Patent No. 6,369,840).

ARGUMENT

A. 35 U.S.C. § 102, Alleged Anticipation, Claims 1-4, 7-16, and 19-24

The Office Action rejects claims 1-4, 7-16, and 19-24 under 35 U.S.C. § 102(e) as being allegedly anticipated by Qian et al. (U.S. Publication No. 2002/0032731). This rejection is respectfully traversed.

As to claim 1, the Office Action states:

> Per claim 1, Qian teaches a method in a data processing system for removing information, the method comprising:
> receiving a selection of confidential information for removal from a history (e.g., cookies) generated by a browser, wherein the selection is received prior to a browser session (col. 2, [0017]; col. 3, [0047]; col.5, [0067], and [0071]); and wherein the history is composed of multiple data elements generated by a browser (col. 5, [0072]);
> identifying data elements within the history, that correspond to the confidential information that has been selected (col. 5, [0067], and [0071]); and
> responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history (col. 2, [0017]; col. 5, [0067], and [0071]).

Final Office Action dated August 18, 2005, pages 2-3.

Claim 1, which is representative of the other rejected independent claims 11, 13 and 23 with regard to similarly recited subject matter, reads as follows:

> 1. A method in a data processing system for removing information, the method comprising:
> receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;
> identifying data elements, within the history, that correspond to the confidential information that has been selected; and
> responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

Qian fails to teach receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser; identifying data elements, within the history, that correspond to the confidential information that has been selected; and responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

Qian is directed to a group-browsing system that masks the identity of each client computer to prevent web sites from retrieving any client's actual identification information that is not part of a group browsing session. The group browsing system may create a temporary identifier for use by each client in a group during a group browsing session, so that, when each such client logs on to a web site, the same web page is displayed for all the clients in the group. At the end of a group-browsing session, the temporary identifiers are automatically discarded to prevent any user from returning to the web site while masquerading as another client.

Thus, Qian teaches creating temporary identifiers for each user during a group browsing session and deletes the temporary identifiers at the end of the group browsing session. Qian does not teach receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session. The Final Office Action alleges that these features are taught by Qian at paragraphs [0017], [0047], [0067], and [0071], which read as follows:

> [0017] Each of the above objects is separate and need not be addressed by every embodiment described herein or every claim. Accordingly, one embodiment addresses at least one of the above objectives by providing a group-browsing system that masks the identity of each client computer to prevent web sites from retrieving any clients actual identification information (e.g., in the form of a cookie) that is not part of a group browsing session. Nonetheless, the group browsing system may create a temporary identifier (e.g., temporary cookie) for use by each client in a group during a group browsing session so that when each such client logs on to a web site the same web page is displayed for all the clients in the group. At the end of a group-browsing session, the temporary identifiers are automatically discarded to prevent any user from returning to the web site while masquerading as another client.

> [0047] Using at least one computer code device on a client-side computer, a user is prompted to authenticate himself/herself (e.g., using a dialog box as shown in FIG. 2A). In one embodiment, a user sends a username and password to a coordination server 12 (discussed below), where the username and password are compared against entries accessible by the coordination server. Such entries may be stored in files, databases or other data repositories. In an alternate embodiment, tokens or time synchronized control words are utilized for authentication.

> [0067] As described herein, a portion of the responsibility of the proxy 70 is to manage cookies between the users of a group. Although a group browsing session preferably starts with no cookies, cookies can be added during the group browsing session. According to one embodiment of the present invention, the proxy runs trigger routine computer code to manage cookies. An exemplary trigger routine computer code and cookie manager computer code are attached hereto in Appendix I. This prevents any client's actual identification information (i.e., personal information created before the group browsing session) from being disclosed. Furthermore, the proxies 70A and 70B are configured to create the same temporary identifier for each client when any client logs on to the web site so that the same web page is displayed for all the clients in the group. An exemplary log that is created by the co-browsing routine which manages the cookies containing an example of temporary identifier is attached hereto in Appendix II.

> [0071] The group-browsing system of the subject invention also prevents any client, identified as another client, from returning to the web site by deleting the temporary identifier at the end of a group-browsing session. Additionally, when other clients in the group are able to access that client's private information, the system generates a warning message. At the end of a group-browsing session, client software is able to detect the end of a group-browsing session and, in response, to direct a client's secure browser to transmit the web site URL, allowing the client to return to the previously accessed web site.

In paragraph 17, Qian describes a group-browsing system that masks the identity of each client computer to prevent web sites from retrieving any client's actual identification information that is not part of a group browsing session. The group browsing system may create a temporary identifier, such as a temporary cookie, for use by each client in a group during a group browsing session so that when each such client logs on to a web site the same web page is displayed for all the clients in the group. At the end of a group-browsing session, the temporary identifiers are automatically discarded. Thus, the selection of confidential information for removal from a history generated by a browser is not selected prior to the browser session. In paragraph 47, Qian describes prompting a use to authenticate himself or herself. In paragraph 67, Qian

describes managing cookies between the users of a group. The group browser session starts **with no cookies.** Thus, the user could not select confidential information for removal from a history generated by a browser **prior** to the browser sessions; because Qian describes the nonexistence of cookies at the **start** of the group browser session. In paragraph 71, Qian describes preventing any client, identified as another client, from returning to the web site by deleting the **temporary identifier at the end of a group-browsing session.** Thus, Qian describes **starting with no cookies and ending with no cookies.** Therefore, Qian does not teach receiving a selection **prior to a browser session** of confidential information for removal from a history generated by a browser.

Additionally, Qian does not teach identifying data elements, within the history, that correspond to the confidential information that has been selected. The Final Office Action alleges that these features are taught in paragraphs [0067] and [0071], shown above. As discussed above, in paragraph 67, Qian describes **starting** a group browser session **with no cookies.** In paragraph 71, Qian describes **ending** of a group-browsing session **with no cookies.** Thus, the system of Qian deletes only those temporary identifiers that it creates **during** the group browser session. Qian fails to teach identifying data elements, within the history, that correspond to the confidential information that has been selected **prior to the browser session.**

Furthermore, Qian fails to teach responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history. The Final Office Action alleges these features are taught at paragraphs [0017], [0067], and [0071], shown above. As discussed above, in paragraph 17, Qian describes creating temporary identifiers for users during a group browsing session and ending the group browsing session by automatically deleting any temporary identifiers that were created during the group browser session. In paragraph 67, Qian describes **starting** a group browser session **with no cookies** and in paragraph 71, Qian describes **ending** of a group-browsing session **with no cookies.** Thus, while Qian automatically deleted the temporary identifiers at the end of the session, Qian does not teach automatically removing the selected confidential information that was selected prior to the browser session. Additionally, as Qian ends with no cookies remaining in the browser

session, Qian destroys all of the history, which is in contradiction to the presently claimed invention where only the selected confidential information is removed **without destroying the integrity of other portions of the history.**

Independent claims 8, 12, 20 and 24 recite similar features in their respective claim terminology. Claim 8, which is representative of the other rejected independent claims 12, 20 and 24, recites "receiving a selection of confidential user information for removal from a history generated by a browser, wherein the selection is received **prior to a browser session** and wherein the history is composed of multiple data elements generated by a browser; identifying data elements, within the history, that correspond to the confidential information that has been selected; and responsive to generation of the history, removing the selected confidential information from the history, wherein **only the selected confidential information is removed** without destroying the integrity of other portions of the history."

Thus, Qian fails to teach all of the features in independent claims 1, 8, 11, 12, 13, 20, 23 and 24. At least by virtue of their dependency on claims 1, 8, 13 and 20, Qian fails to teach all of the features of dependent claims 2-4, 6, 7, 9, 10, 14-16, 18, 19, 21 and 22. Accordingly, Appellants respectfully request that the rejection of claims 1-4, 7-16, and 19-24 under 35 U.S.C. § 102(e) not be sustained.

Furthermore, Qian does not teach, suggest or give any incentive to make the needed changes to reach the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement Qian such that a selection of confidential information is received prior to a browser session for removal from a history generated by a browser, data elements are identified, within the history, that correspond to the confidential information that has been selected prior to the browser session, and, responsive to a termination of the browser session, the selected confidential information is automatically removed from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history, one of ordinary skill in the art would not be led to modify Qian to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion or incentive to modify Qian in this manner, the presently claimed invention can be reached only

through an improper use of hindsight using the Appellant's disclosure as a template to make the necessary changes to reach the claimed invention.

B. **35 U.S.C. § 103, Alleged Obviousness, Claims 6 and 18**

The Office Action rejects claims 6 and 18 under 35 U.S.C. § 103(a) as being unpatentable over Qian et al. (U.S. Publication No. 2002/0032731) and Barnett et al. (U.S. Patent No. 6,369,840). This rejection is respectfully traversed.

Claims 6 and 18 are dependent on independent claims 1 and 13 and, thus, these claims distinguish over Qian for at least the reasons noted above with regards to claims 1 and 13. Moreover, Barnett does not provide for the deficiencies of Qian and, thus, any alleged combination of Qian and Barnett would not be sufficient to reject independent claims 1 and 13 or claims 6 and 18 by virtue of their dependency. That is, Barnett does not teach or suggest receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser; identifying data elements, within the history, that correspond to the confidential information that has been selected; and responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

In view of the above, Appellants respectfully submit that Qian and Barnett, taken alone or in combination, fail to teach or suggest the features of claims 1 and 13. At least by virtue of their dependency on claims 1 and 13, the features of dependent claims 6 and 18 are not taught or suggested by Qian and Barnett, whether taken alone or in combination. Accordingly, Appellants respectfully request that the rejection of claims 6 and 18 under 35 U.S.C. § 103(a) not be sustained.

CONCLUSION

In view of the above, Appellants respectfully submit that claims 1-4, 6-16, and 18-24 are allowable over the cited prior art and that the application is in condition for allowance. Accordingly, Appellants respectfully request the Board of Patent Appeals and Interferences to not sustain the rejections set forth in the Final Office Action.

Francis Lammes
Reg. No. 55,353
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method in a data processing system for removing information, the method comprising:

receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;

identifying data elements, within the history, that correspond to the confidential information that has been selected; and

responsive to a termination of the browser session, automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

2. The method of claim 1, wherein the confidential information includes at least one of a phone number, a credit card number, a social security number, an address of a user, a user identification, a password, and a personal identification number.

3. The method of claim 1, wherein the receiving step comprises:

receiving the selection of confidential information as a user input.

4. The method of claim 3, wherein the user input is received through a graphical user interface.

6. The method of claim 1, wherein the history includes a cookie file, a cache for storing data associated with Web pages, a location list, and a history list.

7. The method of claim 1, wherein the confidential information is received as at least one string.

8. A method in a data processing system for removing information from a history generated by a browser, the method comprising:

receiving a selection of confidential user information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;

identifying data elements, within the history, that correspond to the confidential information that has been selected; and

responsive to generation of the history, removing the selected confidential information from the history, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

9. The method of claim 8, wherein the removing step occurs when a browser session is terminated.

10. The method of claim 8, wherein the confidential user information includes at least one a phone number, a credit card number, a social security number, an address of a user, a user identification, a password, and a personal identification number.

11. A data processing system comprising:

a bus system;

a communications unit connected to the bus system;

a memory connected to the bus system, wherein the memory includes a set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser; identifying data elements, within the history, that correspond to the confidential information that has been selected; and automatically remove the selected confidential information from the history without requiring further user input upon termination of the browser session in response to a termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

12. A data processing system comprising:

a bus system;

a communications unit connected to the bus system;

a memory connected to the bus system, wherein the memory includes a set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes the set of instructions to receive a selection of confidential user information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and

wherein the history is composed of multiple data elements generated by a browser; identify data elements, within the history, that correspond to the confidential information that has been selected; and remove the selected confidential information from the history in response to generation of the history, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

13. A data processing system for removing information, the data processing system comprising:

receiving means for receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;

identifying means for identifying data elements, within the history, that correspond to the confidential information that has been selected; and

automatically removing means, responsive to a termination of the browser session, for automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

14. The data processing system of clam 13, wherein the confidential information includes at least one of a phone number, a credit card number, a social security number, an address of a user, a user identification, a password, and a personal identification number.

15. The data processing system of claim 13, wherein the receiving means comprises:

means for receiving the selection of confidential information as a user input.

16. The data processing system of claim 15, wherein the user input is received through a graphical user interface.

18. The data processing system of claim 13, wherein the history includes a cookie file, a cache for storing data associated with Web pages, a location list, and a history list.

19. The data processing system of claim 13, wherein the confidential information is received as at least one string.

20. A data processing system for removing information from a history generated by a browser, the data processing system comprising:

receiving means for receiving a selection of confidential user information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;

identifying means for identifying data elements, within the history, that correspond to the confidential information that has been selected; and

removing means, responsive to generation of the history, for removing the selected confidential information from the history, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

21. The data processing system of claim 20, wherein the removing means occurs when a browser sessions terminated.

22. The data processing system of claim 20, wherein the confidential user information includes at least one of a phone number, a credit card number, a social security number, an address of a user, a user identification, a password, and a personal identification number.

23. A computer program product in a computer readable medium for removing information, the computer program product comprising:

first instructions for receiving a selection of confidential information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;

second instructions for identifying data element, within the history, that correspond to the confidential information that has been selected; and

third instructions, responsive to a termination of the browser session, for automatically removing the selected confidential information from the history without requiring further user input upon termination of the browser session, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

24. A computer program product in a computer readable medium for removing information from a history generated by a browser, the computer program product comprising:

first instructions for receiving a selection of confidential user information for removal from a history generated by a browser, wherein the selection is received prior to a browser session and wherein the history is composed of multiple data elements generated by a browser;

second instructions for identifying data element, within the history, that correspond to the confidential information that has been selected; and

third instructions, responsive to generation of the history, for removing the selected confidential information from the history, wherein only the selected confidential information is removed without destroying the integrity of other portions of the history.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.